

10/582077

AP3 Rec'd PCT/PTO 08 JUN 2005

Reply Regarding Second Amendment according to Article 34

5. Subject matter of Reply

The International Searching Authority's written opinion notified us that the inventive step of each of Claims 1 to 41 of the present invention is denied based on References 1 (JP2001-285283A), 2 (JP11-341040A) and 3 (JP2001-127785A).

In response to your written opinion, we amend Claims 1 and 40 in order to clarify the features of the present invention by filing the Amendment of Proceedings and this Reply at the same time. This Amendment is based on the descriptions in paragraphs [0095] to [0097] in the Description, and thus no new matters are added.

The features of the present invention are as described in the following Claim 1:

[1] A packet transmitter apparatus which transmits packet data to a packet receiver apparatus, said transmitter apparatus comprising:

- an audio and video (AV) data information obtainment unit operable to obtain AV data information including: input terminal information indicating a terminal to which AV data is inputted; data format information indicating a data format of the AV data; and attribute information indicating an attribute of the AV data;

- a data input unit operable to receive the AV data and non-AV data;

- a transmitting condition setting management unit operable to extract at least one of charge information, playback control information and copy control information of the AV data, from the non-AV data or the AV data, and generate, based on the extracted information, encryption mode information indicating an encryption mode which serves as a condition at the time when the AV data is transmitted;

- an encrypted data generation unit operable to generate encrypted data by encrypting, based on transmitting conditions, the AV data received by said data input unit, and adding encryption information headers based on the

encryption mode information to the encrypted AV data, the transmitting conditions being determined as a combination of the input terminal information, the data format information and the attribute information;

a packet generation unit operable to generate packets by adding packet headers to the encrypted data generated by said encrypted data generation unit;

an authentication unit which performs authentication processing for encryption or decryption of the AV data with the packet receiver apparatus using Uniform Resource Identifier (URI) information indicating an access position of the AV data in the packet transmitter apparatus or extended URI information;

a transmission protocol determination unit operable to determine a transmission protocol of the AV data between said packet transmitter apparatus and said packet receiver apparatus, using at least one of the input terminal information, the attribute information and information indicating a transmission mode specified by said packet receiver apparatus; and

a transmission unit operable to transmit the packets including the encrypted data generated by said packet generation unit to said packet receiver apparatus according to the transmission protocol determined by said transmission protocol determination unit, after the authentication processing with said packet receiver apparatus is completed.

With this configuration, the authentication unit performs authentication processing for encrypting or decrypting the AV data with the packet receiver apparatus using URI information or extended URI information (such as an IP address and a port number). Therefore, it becomes possible to control the authentication processing using general information indicating where the AV data is present. This provides an effect that a special mechanism for controlling such authentication processing becomes unnecessary. For example, in the case where URI is extended by a Query format, it becomes possible to provide information indicating the necessity of authentication and provide the Query information indicating a TCP port number for authentication. This enables to determine an authentication execution mode according to control information inputted from outside, and thus it becomes possible to realize

flexible and various types of copyright protection (The Description, paragraph [0032] and the like).

On the other hand, Reference 1 discloses a technique of transmitting AV data in a form of IP packets while protecting the copyright of the AV data. Indeed, Reference 1 is the same as the present invention in this point.

However, Reference 1 does not disclose or suggest an authentication unit, which is unique in the present invention, in other words, authentication processing using URI information or extended URI information. This is true of the remaining References 2 and 3.

Therefore, we believe that the inventive step of the present invention which includes such unique authentication processing unit is not denied based on these References 1 to 3.

The applicants respectfully request that the above reply be reviewed.

答 弁 書

特許庁審査官 殿

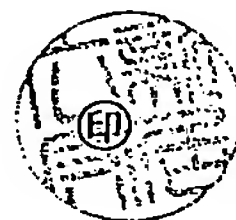
1. 国際出願の表示 PCT/J P 2004/018491

2. 出願人

名称 松下電器産業株式会社
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.
あて名 〒571-8501 日本国大阪府門真市大字門真1006番地
1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501 Japan
国籍 日本国 Japan
住所 日本国 Japan

3. 代理人

氏名 (10921) 弁理士 新居広守
NII Hiromori
あて名 〒532-0011 日本国大阪府大阪市淀川区西中島3丁目11番26号
新大阪末広センタービル3F 新居国際特許事務所内
c/o NII Patent Firm, 3rd Floor, Shin-Osaka Suehiro Center Bldg.,
11-26, Nishinakajima 3-chome, Yodogawa-ku, Osaka-shi, Osaka
532-0011 JAPAN



4. 通知の日付 10.01.2006

5. 答弁の内容

本願請求項1～41に対し、国際調査機関の見解書において、文献1 (JP2000-287192A)、文献2 (JP2000-332745A)、及び、文献3 (JP2000-59323A) に基づいて進歩性が否定される旨の通知を受けました。

これに対し、本答弁書と同時に提出する手続補正書によって、本願発明の特徴を明確にするために、請求項1及び40を補正しました。この補正は、明細書の段落【0095】～【0097】等の記載に基づくものであり、新規事項を追加するものではありません。

本願発明は、請求項1に記載されているように、パケット受信装置にパケットデータを送信するパケット送信装置であって、AVデータが入力される端子を示す入力端子情報、前記

A Vデータのデータフォーマットを示すデータフォーマット情報及び前記A Vデータの属性を示す属性情報を含むA Vデータ情報を取得するA Vデータ情報取得手段と、前記A Vデータ及び非A Vデータの入力を受け付けるデータ入力手段と、前記非A Vデータまたは前記A Vデータより、前記A Vデータの課金情報、再生制御情報及びコピー制御情報の少なくとも1つの情報を抽出し、抽出した情報から、前記A Vデータを送信する際の条件となる暗号化モードを示す暗号化モード情報を生成する送信条件設定管理手段と、前記入力端子情報、前記データフォーマット情報及び前記属性情報を組み合わせて決定される送信条件に基づいて、前記データ入力手段より入力された前記A Vデータを暗号化し、暗号化された前記A Vデータに対して前記暗号化モード情報に基づく暗号化情報ヘッダを付加することによって暗号化データを生成する暗号化データ生成手段と、前記暗号化データ生成手段により生成された暗号化データに対して、パケットヘッダを付加することによってパケットを生成するパケット化手段と、前記A Vデータの前記パケット送信装置内でのアクセス位置を示すURI (Uniform Resource Identifier) 情報または拡張URI 情報を用いて、前記パケット受信装置との間で前記A Vデータの暗号化または復号化のための認証処理を行う認証手段と、前記入力端子情報、前記属性情報及び前記パケット受信装置より指定される送信モードを示す情報の少なくとも1つを用いて、前記パケット送信装置と前記パケット受信装置の間での前記A Vデータの伝送プロトコルを決定する伝送プロトコル決定手段と、前記認証処理によって前記パケット受信装置との認証処理が完了した後に、前記伝送プロトコル決定手段によって決定された伝送プロトコルに従って、前記パケット化手段によって生成された暗号化データを含むパケットを前記パケット受信装置に伝送する伝送手段とを備えることを特徴とします。

このような構成によって、認証手段は、URI 情報または拡張URI 情報（例えば、IPアドレスおよびポート番号）を用いて、パケット受信装置との間でA Vデータの暗号化または復号化のための認証処理を行うので、A Vデータの所在を示す一般的な情報を用いて認証処理を制御することが可能となり、認証処理を制御するための特殊なしくみが不要になるという効果があります。たとえば、URI がQuery形式により拡張されている場合には認証が必要であるという情報と、同時に、そのQuery 情報より認証用のTCPポート番号の情報を与えることが可能となります。これにより、認証実行モードを、外部より入力される制御情報によって決定することができ、柔軟性に富んだ著作権保護が実現されます（明細書の段落【0032】等）。

これに対し、文献1は、A Vデータに対して著作権を保護しつつIPパケットで送出する技術を開示しています。確かに、この点で、本願発明と共通します。

しかしながら、文献1は、本願発明の特徴的な認証処理手段、つまり、URI 情報または拡張URI 情報を用いた認証処理については開示も示唆もしていません。このことは、他の

文献 2 及び文献 3 についても同じです。

よって、特徴的な認証処理手段を備える本願発明は、文献 1 ～ 3 に基づいて進歩性が否定されることはない、と確信します。

以上